Course Syllabus

Computer Science and Engineering

CS9223-Mobile Security

Course Information

Course Prerequisites

- Undergraduate level knowledge of computer systems and networks. ● Owning a smart mobile device, such as a smart phone, will provide an added advantage.
- Knowledge of Operating Systems (such as from 6233) and Security (such as from 6813)

Course Description

Mobile devices are everywhere. While the concept of a mobile device is not new, recent advancements in connectivity, processing power and power storage has allowed mobile devices to displace traditional desktops as the primary means of computing. Today's smartphones can effectively do everything that older desktop computers do (think of the Samsung Dex Docks) and yet are completely portable. Not surprisingly, smartphones and other mobile devices have been the target of cyber criminals since their inception. This, in itself, should not be a surprise and we should already be fully ready to analyze and understand the security implications and issues.

This special topics course is designed to give the student a little bit more insight on how to apply the basic principles of security learned in previous courses to the world of mobile security. If previous courses were more focused on theory, this one is more on practice -- security as practiced in the mobile environment.

The mobile "environment" starts with discussions on the communications infrastructure such as the evolution from GSM (2G), UMTS (3G) and LTE (4G) to the 5G specifications that are being rolled out, then on mobile platforms including iOS and Android, and then to applications and the new design methodologies such as a smaller screen (therefore one App is displayed at a time, while most others are running in the background) or even no screen at all (such as in Internet of Things devices) that must be considered.

The common theme that all students should see is that security is *not* the most important factor, it is often less important than things like "performance." When it comes to security in practice, balance between cost, performance, security, etc. is paramount.

Course Structure

The course consists of core topics (see Weekly Structure below) that are taught using presentations and pre-recorded lectures.

Additionally, this is a high-level graduate course that is meant to reinforce the student's ability to do independent learning on a new and/or up-and-coming topic of interest. Therefore, the main focus will be on "independence". Since one of the major tenets of education is that you don't truly understand something until you can teach it, this course will require students to present the most recent material on the topic of mobile security to the entire class. Students are then required to ask insightful questions and participate.

Grading Breakdown

- 20% Homework Assignments
- 30% Research Paper Presentation / Online Participation
- 30% Project and Project Presentation
- 20% Final Exam / Presentation

Weekly Structure

The core course topics are presented as presentations and pre-recorded lectures. The student is expected to watch the lectures prior to each week's live session.

1. Introduction to Mobile Security

2. Building Blocks – Basic security and cryptographic techniques.

3. Security of GSM Networks

4. Security of UMTS Networks

5. LTE Security

6. WiFi and Bluetooth Security

7. SIM/UICC Security

8. Mobile Malware and App Security

9. Android Security Model

10. IOS Security Model

11. Security Model of the Windows Phone

12. SMS/MMS, Mobile Geolocation and Mobile Web Security. 13.Security of Mobile VoIP Communications

13. Emerging Trends in Mobile Security

Readings

The required text for the course is: *Security of Mobile Communications*, Noureddine Boudriga, 2010

An optional and recommended text is: *Mobile Application Security,* Himanshu Dviwedi, Chris Clark and David Thiel, 1st Edition

Course Load

The course has four homework assignments, one test (see below), one project and two research paper presentations. In the interest of following the mobile trend, we will allow for live presentations from the students as well as posting videos and have question and answer sessions (in the form of comments and responses) on the go. This course will be run in the graduate style where students are encouraged to be independent, take initiative and explore new topics on their own. This should come naturally as part of the homework assignments and research paper presentations.

Homework Assignments

The homework assignments will consist of a series of questions for you to answer. Students have the option of answering the questions in the traditional written format, an audio (e.g., podcast) format or a video (e.g., vlog). Please keep in mind that while you might not be graded on style or production value, this is an opportunity for you to get practice in any of the three communications methods without judgment.

Final Exam

The final exam will assess your knowledge and mastery over the lecture material. We might forego with the final exam as well depending on the quality and sophistication of the projects.

Research Paper Presentations

Each student will be required to pick two research papers, summarize them and then record themselves presenting the paper as if they were presenting it at a conference. Alternatively, the student can choose to present live to the entire class.

A good place to start is USENIX Security https://www.usenix.org/conference/usenixsecurity19 which just took place in August. They have a mobile track, so it is a good place for you to find research papers. They also record all of the presentations so you have a good idea on what the presentations should look like.

Make sure you don't plagiarize their presentations

Project

The project has to be conducted in teams of three. For the project, you will pick a topic - the project might involve experimentation, coding, simulation or anything of your choosing - that highlights a new principle or characteristic of mobile security that did not exist prior. All research topics must be approved by the instructor. In order to facilitate this, team are required to submit a two page "whitepaper" by the end of the 3rd week (earlier is fine). Then, the students will submit a detailed project report by the end of the semester.

Lectures

Pre-recorded lecture material is provided to the student as a quick overview. Students are expected to listen to the lecture material on a weekly basis. We will also be conducting live sessions so we can have any questions answered, issues addressed, and additional topics discussed. The live sessions will also serve as a forum for project updates and meetings.

Schedules

The exact dates and schedules will be determined during the first couple of weeks as it depends on the number of students enrolled.

Student Responsibilities

- **Online lectures:** Each lecture will consist of slides and video lectures. You are expected to read the relevant material in the textbook, and follow the video lectures.
- You are required to check online site daily for: information, announcements, discussions, updated lecture notes, assignments, reading material etc.
- **Late Policy:** Submit assignments and tests on time - no extensions will be granted.

Interaction Policy

- Live sessions will be held weekly on WebEx/Zoom. Please join if available.
- Questions will be answered via email or through the virtual classroom sessions. For additional questions and interaction, please schedule an appointment.

University Policies

Academic Integrity Policy (Does not supercede University Policy)

Students must behave ethically at all times. All work should represent the students' original ideas and thoughts. When doing the assignment you may consult any relevant source or person, but if you take information in a substantial way from someone or somewhere, you should reference it. You are NOT allowed to copy code/content in ANY FORM from any source. All tests will be individual and open book, but timed, and you may not consult anyone during the test. Any violation of the academic integrity policy will be awarded ZERO points.

Moses Center Statement of Disability

Academic accommodations are available for students with disabilities. Please contact the Moses Center for Students with Disabilities (212-998-4980 or mosescsd@nyu.edu) for further information. Students who are requesting academic accommodations are advised to reach out to the Moses Center as early as possible in the semester for assistance.

NYU Tandon School of Engineering Policies and Procedures on Academic Misconduct[1]

A. Introduction: The School of Engineering encourages academic excellence in an environment that promotes honesty, integrity, and fairness, and students at the School of Engineering are expected to exhibit those qualities in their academic work. It is through the process of submitting their own work and receiving honest feedback on that work that students may progress academically. Any act of academic dishonesty is seen as an attack upon the School and will not be tolerated. Furthermore, those who breach the School's rules on academic integrity will be sanctioned under this Policy. Students are

[1] Excerpted from the Tandon School of Engineering Student Code of Conduct

responsible for familiarizing themselves with the School's Policy on Academic Misconduct.

B. Definition: Academic dishonesty may include misrepresentation, deception, dishonesty, or any act of falsification committed by a student to influence a grade or other academic evaluation. Academic dishonesty also includes intentionally damaging the academic work of others or assisting other students in acts of dishonesty. Common examples of academically dishonest behavior include, but are not limited to, the following:

    a. Cheating: intentionally using or attempting to use unauthorized notes, books, electronic media, or electronic communications in an exam; talking with fellow students or looking at another person's work during an exam; submitting work prepared in advance for an in-class examination; having someone take an exam for you or taking an exam for someone else; violating other rules governing the administration of examinations.

    b. Fabrication: including but not limited to, falsifying experimental data and/or citations.

    c. Plagiarism: intentionally or knowingly representing the words or ideas of another as one's own in any academic exercise; failure to attribute direct quotations, paraphrases, or borrowed facts or information.

    d. Unauthorized collaboration: working together on work that was meant to be done individually.

    e. Duplicating work: presenting for grading the same work for more than one project or in more than one class, unless express and prior permission has been received from the course instructor(s) or research adviser involved.

    f. Forgery: altering any academic document, including, but not limited to, academic records, admissions materials, or medical excuses.

NYU School of Engineering Policies and Procedures on Excused Absences

A. Introduction: An absence can be excused if you have missed no more than 10 days of school. If an illness or special circumstance has caused you to miss more than two weeks of school, please refer to the section labeled Medical Leave of Absence

B. Students may request special accommodations for an absence to be excused in the following cases:
   a. Medical reasons
   b. Death in immediate family
   c. Personal qualified emergencies (documentation must be provided)
   d. Religious Expression or Practice